PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :		(11) International Publication Number:
H04K 1/00, H04L 9/00, G06F 17/60	A1	WO 97/50205
		(43) International Publication Date: 31 December 1997 (31.12.97)

(21) International Application Number: PCT/US97/10292

(22) International Filing Date: 11 June 1997 (11.06.97)

(30) Priority Data:
08/678,360 26 June 1996 (26.06.96) US

(71) Applicant: INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

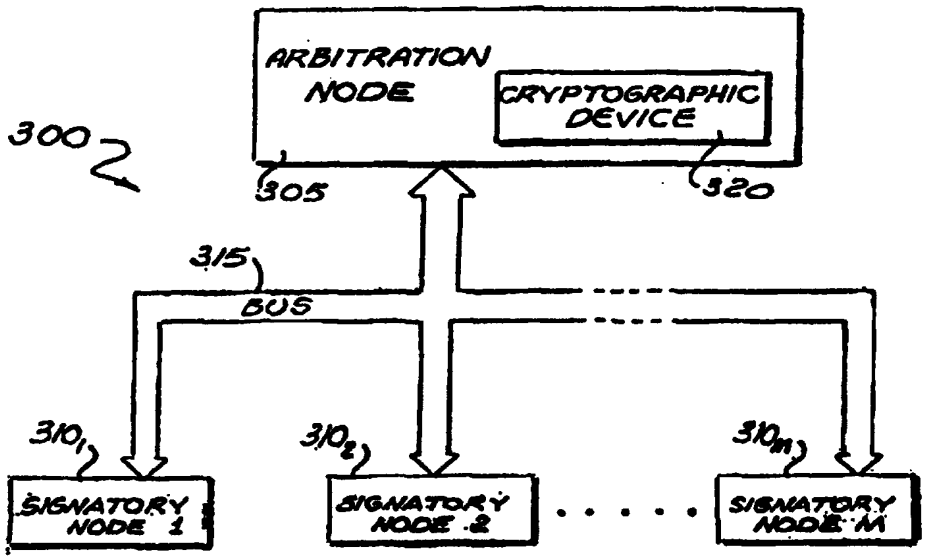
(72) Inventor: DAVIS, Derek, L.; 4509 E. Desert Trumpet Road, Phoenix, AZ 85044 (US).

(74) Agents: TAYLOR, Edwin, H. et al.; Blakely, Sokoloff, Taylor & Zafman LLP, 7th floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 (US).

(81) Designated States: AL, AM, AT, AT (Utility model), AU (Petty patent), AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: DIGITALLY SIGNING AGREEMENTS FROM REMOTELY LOCATED NODES



(57) Abstract

A digital arbitration system comprising a server node and at least one signatory node (310) coupled together through a communication link (315). Each of the signatory node(s) may be configured to include a unique private key which is used to digitally sign a message, a hash value of an electronic document for example, and transmits the digitally signed message, being a digital signature, to the server node via the communication link. The server node (fig. 7) determines whether the digital signatures have been received from at least one the signatory node(s) and whether each of the digital signatures is valid. The server node then transmits all of the digital signatures to each of the signatory node(s), provided both conditions described have been met.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

DIGITALLY SIGNING AGREEMENTS FROM REMOTELY LOCATED NODES

CROSS-REFERENCES TO RELATED APPLICATIONS

The named inventor of the present application has filed a number of co-pending United States Patent Applications entitled "An Apparatus And Method For Performing Secured Cryptographic Operations" (Application No. 08/578,177, a Continuation of Application No. 08/251,486, filed on December 29, 1995), "A Method For Providing Secured Communications" (Application No. 08/538,869, a Divisional of Application No. 08/251,486, filed on October 4, 1995), "A Method For Providing A Roving Software License In A Hardware Agent-Based System" (Application No. 08/472,951, a Divisional of Application No. 08/303,084, filed on June 7, 1995) and "An Apparatus and Method for Securing Captured Data Transmitted Between Two Sources" (Application No. 08/538,189, filed on September 29, 1995). These applications are owned by the same assignee of the present Application.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to the field of communications. More particularly, the present invention relates to a system and method for creating a remote digital agreement formulated through an execution procedure.

2. Description of Art Related to the Invention

Over hundreds of years, written agreements have been used as a vehicle for a variety of purposes, among which is to establish certainty and clarity in business, legal and other types of arrangements between two or more parties to the agreement. In general, one type of an agreement is a "contract", which is defined as a promise or

set of promises between two or more parties by which the law allows the party or parties that abide by the terms of the contract to recover damages (e.g., monetary compensation) from the party or parties that breach the contract. Another type of agreement is a stipulation agreement used during litigation in which the parties agree to material facts not in dispute. Although there exists a wide variety of execution schemes, one type of scheme is where the parties to the contract negotiate "at arm's length" to formulate terms of the written agreement (e.g., contract) which are mutually agreeable to the parties.

After agreeing to the terms of the written agreement, the parties select an execution procedure for signing the agreement. The nature of that execution procedure may depend on the importance of the agreement, past dealings between the parties, and many other factors. The execution procedure may be overseen by a "non-signing party" acting as an arbitrator (referred to as "independently-arbitrated agreement execution"), or by the parties themselves in a localized setting (referred to as "mutually-arbitrated agreement execution").

Referring to **Figure 1**, mutually-arbitrated agreement execution is generally preferred when all of the parties or the signatories of the agreement 110 can meet at a selected location to execute one or more printed copies of the agreement 120. This guarantees that each party possesses an original copy of the agreement upon adjournment of the meeting. Such meetings are costly and difficult to arrange, especially when the agreement involves a large number of parties.

In the event that the simultaneous assembly of all parties is not feasible or undesirable, an alternative approach may include an independently-arbitrated execution procedure utilizing human arbitration as shown in **Figure 2**. For this execution procedure, each signatory 1101 and 1102 separately executes one or more copies of the agreement and provides the partially-signed agreements 1301 and 1302 to the arbitrator 140 (e.g., a third party who is not a signatory of the agreement). When receiving partially-signed agreements 1301 and 1302 from all of the parties, the arbitrator 140 provides a copy of the fully-signed agreement 1501 and 1502 back to each signatory 1101 and 1102. The disadvantage associated with this execution

procedure is that it is entirely dependent on the integrity of the arbitrator 140 to properly follow a static procedure. However, it is apparent that it is quite difficult and costly, especially for parties situated in other countries and/or in different states, to check the integrity of the arbitrator. Likewise, the cost of the arbitration service itself and the time delay in execution of the written agreement may be unacceptable.

Referring now to **Figure 3**, another execution procedure (referred to as "non-arbitrated execution") is applicable when the written agreement is of lesser value or when a sufficient degree of trust exists between the "n" signatories ("n" being a whole number, $n \geq 3$ in this example). One signatory 1101 starts the execution process by signing the agreement and forwarding the partially-signed agreement 1601 on to the next signatory 1102. As each successive signatory receives the partially-signed agreement, it applies its own signature and forwards it to another signatory until the agreement is fully executed. The last signatory 110n has the responsibility to return copies of the fully-executed agreement 1701, 1702, ... 170n1 to all signatories, as did the arbitrator in **Figure 2**. This method has the advantage of cost reduction, since the signatories need not be assembled nor is an arbitration fee incurred. The significant disadvantage is that the success of the process is dependent on the integrity of the last signatory who is a party to the agreement. The last signatory is not compelled to redistribute copies of the signed agreement, especially if a business advantage can be gained by being in possession of the only signed agreement.

Recently, a number of states have passed legislation that recognizes private key-based digital signature as legally binding a party to the terms of a digital agreement. A "digital agreement" is an electronic document representing an agreement that is to be digitally signed by all parties to the agreement through their respective private keys. Like written agreements, digital agreements may be executed through independent-arbitration, mutual-arbitration, or nonarbitration execution procedures. However, it is evident that cost and time saving advantages offered by digital agreements would be greatly reduced by following an independently-arbitrated execution procedure or a mutually-arbitrated execution procedure. Thus, it has been desirable for digital agreements to undergo non-arbitrated execution as shown in **Figure 4**.

Referring to **Figure 4**, after negotiating the terms of the digital agreement 205, a first party at a first node 200 (e.g., computer) normally signs the digital agreement 205 by (i) applying a hash algorithm (e.g., "MD5" algorithm developed by RSA Data Security of Redwood City, California) to the digital agreement 205 to obtain its unique hash value 210, and (ii) encrypting the hash value 210 with an asymmetric cryptographic algorithm (e.g., RSA algorithm) under its private key ("PrKA") to produce a "first digital signature" 215. It is contemplated that such hashing is not necessary, but may be used to reduce the amount of data thereby preserving bandwidth during transmission and memory during storage. Thereafter, at least the first digital signature 215 is transferred to another party at a second node 220. Additional information may be transferred in combination with the first digital signature 215 such as the digital agreement 205 or its hash value 210. Optionally, some or all of this information may be protected during transfer (for privacy purposes) by encrypting with a previously chosen symmetric key.

The execution procedure can be continued in a serial manner by the party at the second node 220 creating its own digital signature 230 (e.g., in this embodiment, hash value 225 encrypted under a private key "PrKB" of the party at the second node 220). Thereafter, an aggregate signature set 235 (including the first and second digital signatures 215 and 230 and possibly additional information) to the next party of the agreement. This procedure may continue for an arbitrary number of parties with the final party at node 240 being responsible for returning the fully-signed digital agreement 250 (i.e., in this case, a hash value of the agreement individually encrypted with the private keys of each party to the digital agreement to all of the other signatories.

Referring now to **Figure 5**, if the first digital signature 215 is created by encrypting the hash value 210 under the private key PrKA, the first digital signature 215 may be validated by any party with access to the hash value 210 (or the original digital agreement 205. Such validation is accomplished by decrypting the first digital signature 215 with a well-known public key ("PuKA") associated with the first party at node 200 to produce a resultant value 260. Thereafter, the resultant value 260 is compared to a previously obtained or computed hash value 210 of the digital

agreement 205 as shown. If the resultant value 260 and the hash value 210 are identical, the first party is deemed to have signed the digital agreement. This procedure may be performed to validate the signature of any of the signatories.

As realized by viewing **Figures 4** and **5**, this nonarbitrated execution procedure for digital agreement clearly poses a risk to all signatories, except the final signatory 240 in the event that the final signatory 240 fails to return a copy of the fully-signed digital agreement to each of the other signatories 200 and 220. For example, if the agreement requires a first signatory to make a monetary payment, to supply goods, or to provide services to the final signatory and the first signatory has not yet received the fully-signed digital agreement from the final signatory, the first signatory risks breaching the agreement if it does not act in accordance with the terms of the agreement. Moreover, if the final party later decides to not abide by the terms of the agreement, the first party may have only limited legal recourse to retrieve its monetary payment or return of its goods. This is due to the fact that the first party only has a copy of a partially-signed digital agreement, not the fully-signed agreement which may have been erased, destroyed, or never signed by the final party. Regardless of the outcome, this non-arbitrated execution procedure allows the business arrangement to be controlled by the final party signing the digital agreement by the accidental or intentional failure to return the fully-signed digital agreement.

In a recent cryptography publication by Bruce Schneier entitled "*Applied Cryptography*" (2nd Edition), an overview is presented of protocols for non-arbitrated, "simultaneous" execution of digital contracts, attempting to address the issue of one signatory to a digital contracts having an advantage over another. These are very tedious, communication intensive protocols, based on each signatory taking a great number of steps in the signature process to build up complete signatures from the other signatories. However, this publication fails to provide a simple protocol for arbitrated execution of digital agreements and a protocol that does not exclusively depend on the integrity of the arbitrator.

Therefore, it would be desirous to create a system and method for reducing the risks associated with execution of digital agreements, while maintaining the cost, time, and convenience advantages of remote execution.

SUMMARY OF THE INVENTION

A digital arbitration system comprising a arbitration node and one or more signatory node(s) coupled together through a communication link. Each of the signatory node(s) may include a unique private key which is used to digitally sign a message, forming a digital signature, and transmit the digital signature over the communication link to the server node. Alternatively, if only one signatory node is used, each party's signature may be created within a removable personal token supplied by that party. The server node transmits an acknowledge signal or the digital signatures from the parties to each of these parties upon receiving all of the digital signatures and determining that each of the digital signatures is valid.

BRIEF DESCRIPTION OF THE DRAWINGS

The features and advantages of the present invention will become apparent from the following detailed description of the present invention in which:

Figure 1 is an illustrative embodiment of a face-to-face meeting of two signatories of an agreement following a mutually-arbitrated agreement execution procedure.

Figure 2 is an illustrative embodiment of a non-signing human arbitrator receiving partially signed agreements from signatories of the agreement and returning fully signed agreements in accordance with an independently-arbitrated agreement execution procedure.

Figure 3 is an embodiment illustrating the normal operations undertaken by a non-arbitrated agreement execution procedure.

Figure 4 is a block diagram of a conventional technique for digitally signing a digital agreement concerning two or more remotely located parties through the use of well-known cryptographic techniques.

Figure 5 is a block diagram of a conventional technique used to verify whether a party has digitally signed the digital agreement.

Figure 6 is a block diagram of a first embodiment of a digital arbitration system.

Figure 7 is a block diagram of an embodiment of the cryptographic device implemented within the arbitration node of the digital arbitration system of **Figure 6**.

Figure 8 is a block diagram of a second embodiment of the digital arbitration system.

Figure 9 is a block diagram of a third embodiment of the digital arbitration system.

Figure 10 is a flowchart illustrating the method of operations of the digital arbitration system of **Figures 6, 8** and **9**.

DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention relates to a system and method for digitally signing a digital agreement between remotely located nodes in a manner which precludes fraudulent withholding of the fully-signed digital agreement in an effort to gain an unfair advantage over a contractual business arrangement. In the following description, numerous details are set forth such as certain configurations of a digital arbitration system in order to provide a thorough understanding of the present invention. It will be obvious, however, to one skilled in the art that other system configurations may be utilized while still practicing the present invention.

In the detailed description, a number of cryptography-related terms are frequently used to describe certain characteristics or qualities which is defined herein. A "key" is an encoding and/or decoding parameter being a sequence of binary data that is used by cryptographic algorithms (e.g., Rivest, Shamir and Adleman "RSA", Digital Signature Standard "DSS", Elliptic Curve, etc.) as public and private key pairs, or used by cryptographic algorithms (e.g., Data Encryption Standard "DES") as a selected "session" key shared in confidence between the two parties. A "message" is digital information, for example, an electronic document or a hash value of one or more electronic document(s) if hashing is utilized. A "digital signature" is digital information resulting from information encrypted with a private key of a party. Such information may include, but is not limited to, an electronic document, a hash value and the like. This digital signing process allows a recipient of the digital signature to verify the identity of the party sending the digital signature. This may be accomplished by decrypting the digital signature with a public key corresponding to the private key of the signing party. A "certificate" is defined as digital information resulting from information, typically a public key associated with the holder of the certificate, encrypted with a private key held by another entity (e.g., manufacturer, arbitration service provider "operator" responsible for the arbitration system, trade association, governmental entity and the like).

Referring to **Figure 6**, a first embodiment of a digital arbitration system is illustrated. The digital arbitration system 300 comprises an arbitration node 305 such as, for example, a computer functioning as a server. The arbitration node 305 is coupled to one or more signatory nodes 3101-310m ("m" ≥ 1 and a whole number) through a communication link 315. The signatory nodes 3101-310m may include any device capable of communicating with the communication link 315 and producing digital signatures. Examples of such devices include, but are not limited to, personal computers, servers, mainframes, workstations, PDAs (personal digital assistants), telephones, etc.

The arbitration node 305 contains a cryptographic device 320 that is capable of operating as a digital arbitrator by collecting digital signatures produced from signatory nodes 3101-310m. The signatory nodes 3101-310m may be owned or controlled by each party of a digital agreement having nodes 3101-310m, or alternatively one signatory node may be controlled with an ability to receive personal tokens (e.g., circuitry configured to securely store one's private key) having a private key associated with the party securely implemented thereon. Thus, one signatory node placed at a centralized location may be used by the parties of the digital agreement.

Thereafter, copies of all of these digital signatures (collectively representing the fully-signed digital agreement) may be returned to each of the parties after certain conditions have been met. It is contemplated that the fully-signed digital agreement may be stored in the arbitration node 305 with acknowledgment signals sent to each of the parties that agreement has been signed by all parties. Copies of the agreement may be requested by any of the signatories or may be sent after signing is completed.

The communication link 315 may be accessible to the public at large (e.g., Internet) or accessible to a lesser number of individuals as in a local area network ("LAN") or a wide area network ("WAN"). This communication link 315 provides bi-directional communications between the arbitration node 305 and the signatory nodes 3101-310m representing one or more parties to the digital agreement so that the arbitration node 305 transmits and receives information to produce a legally

enforceable digital agreement. The procedure undertaken by the arbitration node 305 for exchanging information is discussed below in detail.

Referring to **Figure 7**, the cryptographic device 320 comprises an internal bus 400 interconnecting a processing unit 405, non-volatile memory unit 410, an optional volatile memory unit 415 (as denoted by dashed lines), an optional random number generator 420 (as denoted by dashed lines) and a bus control unit 425. The non-volatile memory unit 405 contains at least the public/private key pair 411 and 412 uniquely associated with the cryptographic device 400. It is contemplated that as arbitration software 413 may be contained within the non-volatile memory unit 405 or may be stored outside the cryptographic device 320, assuming such software its cryptographically protected. When in operation, the arbitration software 413 performs one or more arbitration protocols. The bus control unit 425 controls data transmission between the cryptographic device 400 and the communication link 315, establishing communications with any one of the "m" signatory nodes remotely located from the arbitration node 305.

Optimally, the volatile memory unit 410 may be utilized as temporary storage by the processing unit 405 during execution of arbitration software 413. The random number generator 420 may be used in the initial generation of the public/private key pair 411 and 412 contained in the nonvolatile memory unit 410. It is desirable to implement the random number generator 420 to guarantee that a private key of a unique public/private key pair has not been exposed in readable form outside the cryptographic device 320. Also, the cryptographic engine hardware represented by symmetric (e.g., DES-based) and asymmetric (e.g., RSA-based) encryption/decryption units may be implemented, as indicated by dashed lines, to assist in cryptographic operations.

It is contemplated, however, that the cryptographic device 320 may be implemented in a number of alternative embodiments. For example, the cryptographic device may be implemented with discrete logic on a printed circuit board, or implemented within a chip set operating in cooperation with a host processor. There exist many embodiments which, although slightly different in design, do not deviate

from the spirit and scope of the invention. An example of such an alternative embodiment is illustrated in **Figure 8**.

Referring to **Figure 8**, a second embodiment of the digital arbitration system 500 is illustrated in which the collective cryptographic operations are performed by the arbitration node 505. In contrast to the description of **Figures 6-7**, the arbitration node 505 does not employ the general purpose cryptographic device. Instead, the arbitration node 505 may be implemented with hardware or dedicated to exclusively handle cryptographic arbitration operations.

As shown, the digital arbitration system 500 comprises the arbitration node 505 coupled to a number of signatory nodes 5101-510n through a communication link 515 (e.g., Internet, LAN, WAN, etc.). The arbitration node 505 contains a dedicated hardware arbitration device 520 (e.g., programmable logic devices, state machines, etc.) that primarily performs arbitration functions without being implemented with other general capabilities. The advantage of this type of embodiment is that it may have cost advantages over other embodiments. Once authentication of the dedicated hardware arbitration device 520 is performed (as detailed in following sections), no further authentication is required since the functionality of the arbitration node 505 is not easily modifiable due to its fixed or static hardware implementation.

Referring to **Figure 9**, a third embodiment of the digital arbitration system is illustrated in which the collective cryptographic operations are performed by a computer at a platform level (e.g., host processor, memory, etc.), not by a specific cryptographic device as described in **Figures 7** and **8**. The digital arbitration system 600 comprises the arbitration node 605 coupled to a number of signatory nodes 6101-610m through a communications link 615 (e.g., Internet, LAN, WAN, etc.). The arbitration node 605 is configured with arbitration software stored in memory (e.g., Random Access Memory "RAM", various types of Read Only Memory "ROM", flash memory and the like). The arbitration software is coded to produce similar functionality to that provided the cryptographic device, as shown in **Figure 10** and discussed below, when the host processor is executing instructions associated with the code. However, this implementation does not provide an ability to remotely

authenticate the arbitration software implemented within the arbitration node 605 to guarantee its operation in a manner designated by the parties. Rather, the parties need to rely on the integrity and reputation of the owner or controller of the arbitration node 605.

Referring now to **Figure 10**, the operations of the arbitration node implemented with one of the three embodiments of **Figures 6, 8** and **9** to produce a fully-signed digital agreement are shown. First, in Step 705, the parties can mutually verify that each party is authorized to enter into the digital agreement. This can be accomplished verbally over the phone or, when dealing with business entities, by exchanging a digital certificate signed by a private key ("PrKTA") of a trusted authority (e.g., a partner or officer of the business, security office, etc.). The public key of the trusted authority ("PuKTA") should be widely available or verifiable through additional digital certificates or a digital certificate chain. Then, the parties negotiate the terms and wording of the digital agreement and specify the required signatories, including their public keys (Step 710). Next, the parties seek out and tentatively agree on a digital arbitrator, such as those shown in **Figures 6, 8** and **9** (Step 715). Upon agreeing on a digital arbitrator as shown in **Figures 6** and **8**, the parties check whether the digital arbitrator is implemented with an appropriate and acceptable arbitration mechanism. Otherwise, for a digital arbitrator utilizing only arbitration software as in **Figure 9**, authentication of the arbitration mechanism is not performed, but rather of the owner or operator of the arbitration node. Thus, reliance is placed on the reputation of the owner or controller of the arbitration node (Steps 710-725).

More specifically, in the event that the arbitration node employs a cryptographic device having either a dedicated arbitration functionality as shown in **Figure 8** or general cryptographic functionality configured for arbitration (e.g. via software or firmware) as shown in **Figures 6-7**, authentication of the cryptographic device may be performed by a number of authentication procedures. One authentication procedure is by at least one of the parties requesting the arbitration node's (or cryptographic device's) public key ("PuKARB") and its manufacturer's certificate. Normally, the manufacturer's certificate is a message indicating that the

arbitration node was manufactured by a certain company. Both the manufacturer's certificate and the public key are encrypted with a private key of a reputable manufacturer or trusted authority (e.g., a trade association, governmental entity, etc.) whose public key is widely disseminated. Thus, the parties can obtain PuKARB and send a challenge message to the arbitration node requesting a response to the message, this requested response being the message encrypted with the private key ("PrKARB") of the arbitration node. If the party can read the response by decrypting it with PuKARB, the arbitration node has been authenticated to be the device that the parties have sought.

If a general purpose cryptographic device configured for arbitration via software or firmware is employed within the authentication node of the arbitration system as in **Figures 6-7**, an additional authentication operation may be performed to ensure that an acceptable version of such firmware/software is installed. This authentication operation consists of querying the previously authenticated cryptographic device for details of its configuration. Based on the authenticity and known functionality of the cryptographic device and its firmware/software, a determination is made as to the acceptability of the installed arbitration protocol.

If the arbitration functionality is implemented as software running on the arbitration node under the control of an arbitration service provider, alternative methods of authenticating both the node and its configuration may be required. For example, one technique is to authenticate the node using a "Challenge-Response" authentication technique. Normally, the Challenge-Response authentication technique involves at least one of the parties sending a message requesting an "operator" certificate from the node. The "operator" certificate includes a message indicating that the node is under the control of the arbitration service provider and a public key of the node. Both the message and the public key of the node are encrypted with a private key of the arbitration service provider. The message and public key of the node can be obtained by decrypting the operator certificate with the public key of the arbitration service provider. Thus, authentication of the arbitration node is implicit depending on the reputation of the arbitration service provider who may be legally responsible for the operations of the arbitration node.

Of course, the highest degree of overall execution security and integrity is achieved when each party of the agreement performs these authentication operations and does so in an independent fashion. If the arbitrator authentication cannot be completed, a new digital arbitrator is selected by returning to Step 715.

In Step 730, each signatory digitally signs the digital agreement by encrypting a hash value of the digital agreement or the digital agreement itself (if hashing is not desired) with its private key. This digital signature, along with a signatory list and preferably, although not required, a copy of both the digital agreement or an equally acceptable alternative representation (e.g. hash value of the digital agreement), is then transferred to the digital arbitrator. This communication to the digital arbitrator is confidential, such as being protected through standard cryptographic means, typically by encrypting at least the digital signature with a temporary session key shared between the signatory and the digital arbitrator. This prevents the illicit capture of the digital signature by antagonistic parties, for use prior to the availability of the fully signed digital agreement from the digital arbitrator.

For each individual message received from the various signatories in Step 735, the digital arbitrator performs the operations described in Step 740. These include (i) comparing the received digital agreement (or its acceptable alternative representation) against all versions of the agreement previously received, (ii) comparing the received signatory list against all versions of the signatory list previously received, and (iii) validating the digital signature using the public key of the signatory derived from the signatory list in the manner described for **Figure 5**. As shown in Step 745, the arbitrator must successfully complete all of the operations in Step 740 for all signatories before proceeding.

If valid digital signatures are received from all signatories and all copies of the digital agreement and signatory list are identical, the agreement is deemed to have been fully executed and the arbitrator proceeds to Step 750. In Step 750, the arbitrator distributes an acknowledgment to each signatory indicating that the digital agreement has been fully signed. The digital agreement is contained in the arbitration node to be provided upon request by one of the signatories. Similarly, requests for a copy of the

signatory list, or the set of signatures may be satisfied by the arbitration node. Alternatively, it is contemplated that the entire set of digital signatures associated with the digital agreement may be distributed with or without the use of the session key or asymmetric (public-private key) cryptography techniques.

The present invention described herein may be designed in many different methods and using many different configurations. For example, the present invention may be utilized by escrow companies or other financial institutions for arbitrating the exchange of wired monetary payments for records of title (e.g., deed). Another example would be the remote electronic mutual stipulation to a set of facts as might occur in a judiciary proceeding. Likewise, it could be used by any state or federal regulated entities (e.g., Department of Motor Vehicles). While the present invention has been described in terms of various embodiments, other embodiments may come to mind to those skilled in the art without departing from the spirit and scope of the present invention. The invention should, therefore, be measured in terms of the claims which follows.

CLAIMS

What is claimed is:

1. A digital arbitration system comprising:

a communication link;

a plurality of signatory nodes coupled to said communication link, each of said plurality of signatory nodes (i) includes at least a unique private key which can be used to digitally sign a message, and (ii) is configured to transmit said digitally signed message over said communication link; and

a server node coupled to said communication link, said server node is configured to determine whether each of said plurality of digitally signed messages have been received from said plurality of signatory nodes, to determine whether each of said plurality of digitally signed messages is valid, and to transmit said plurality of digitally signed messages to each of said plurality of signatory nodes if each of said plurality of messages has been received and is valid.

2. The digital arbitration system according to claim 1, wherein said message is one of an electronic document and a hash value of said electronic document.

3. The digital arbitration system according to claim 1, wherein at least one of said plurality of signatory nodes further transmits a list of signatories associated with said message.

4. The digital arbitration system according to claim 3, wherein each of said plurality of signatory nodes further transmits a copy of said message.

5. The digital arbitration system according to claim 1, wherein said arbitration node includes a unique public key and private pair to enable at least one of said plurality of signatory nodes to authenticate said server first node.

6. The digital arbitration system according to claim 1, wherein each of said plurality of signatory nodes is a computer.

7. The digital arbitration system according to claim 6, wherein said server node is a computer including a cryptographic device which can validate each of said plurality of digitally signed messages.

8. The digital arbitration system according to claim 7, wherein said cryptographic device of said server node includes

an internal bus;

a processing unit coupled to said internal bus; a memory element coupled to said internal bus,

said memory element contains at least a public key, a private key and arbitration software; and

a bus control unit coupled to said bus and said internal bus.

9. The digital arbitration system according to claim 8 further comprising a random number generator coupled to said internal bus.

10. The digital arbitration system according to claim 8 further comprising at least one cryptographic engine.

11. The digital arbitration system according to claim 6, wherein said server node is a computer including a memory element containing software and a processor executing said software to at least validate each of said plurality of digitally signed messages.

12. The digital arbitration system to claim 6, wherein said server node is a computer including a cryptographic device dedicated to exclusively operate as an arbitrator between said plurality of signatory nodes.

13. A digital arbitration system to sign a digital agreement comprising:

a communication link;

at least one signatory node coupled to said communication link, said at least one signatory node (i) receives at least one unique private key from each party of the digital agreement which can be used to digitally sign a message, and (ii) is configured to transmit said digitally signed message over said communication link; and

an arbitration node coupled to said communication link, said arbitration node is configured to determine whether a plurality of digitally signed messages, corresponding in number to the parties of the digital agreement, have been received from said at least one signatory node, to determine whether each of said plurality of digitally signed messages is valid, and to transmit said plurality of digitally signed messages to said at least one signatory node if each of said plurality of digitally signed messages has been received and is valid.

14. The digital arbitration system according to claim 13, wherein each party of the digital agreement has a unique private key implemented on a removable personal token.

15. A digital arbitration system comprising:

link means for communicating information;

first signatory node means for digitally signing a

message to form a first digital signature and for transmitting said first digital signature over said link means;

second signatory node means for digitally signing a message to form a second digital signature and for transmitting said second digital signature over said link means;

server means for receiving said first and second digital signatures, for determining whether said first and second digital signatures are valid, and for transmitting said first and second digital signatures to both said first and second signatory node means if said first and second digital signatures are valid.

16. The digital arbitration system according to claim 15, wherein said first digital signature is one of an electronic document and a hash value of said electronic document encrypted with a private key of said first signatory node means.

17. The digital arbitration system according to claim 16, wherein said second digital signature is one of said electronic document and said hash value of said electronic document encrypted with said private key of said second signatory node means.

18. The digital arbitration system according to claim 17, wherein at least one of said first and second signatory node means further transmits a list of signatories along with its corresponding digital signature.

19. The digital arbitration system according to claim 18, wherein at least one of said first and second signatory node means further transmits a copy of said message.

20. The digital arbitration system according to claim 18, wherein said server means includes a computer comprising cryptographic device to validate each of said first and second digital signatures.

21. The digital arbitration system according to claim 20, wherein said cryptographic device includes

an internal bus;

a processing unit coupled to said internal bus;

a memory element coupled to said internal bus,

said memory element contains at least a public key and, a private key; and

a bus control unit coupled to said link means and said internal bus.

22. The digital arbitration system according to claim 21, wherein said cryptographic device includes a random number generator coupled to said internal bus.

23. The digital arbitration system according to claim 18, wherein said server means includes a computer comprising a memory element that contains arbitration software and a host processor that executes instructions from the arbitration software to at least validate said first and second digital signatures.

24. A method for signing a digital agreement between a plurality of parties being arbitrated by a server node, the method comprising the steps of:

1) receiving a plurality of digital signatures, each digital signature of said plurality of digital signatures is unique and corresponds to one of the plurality of parties;

2) validating each of said plurality of digital signatures through a plurality of cryptographic operations; and

3) transmitting said plurality of digital signatures to each party of the plurality of parties to the digital agreement upon satisfying the conditions of steps (1) and (2).

25. The method according to claim 24, wherein said validating step is performed on each of said plurality of digital signatures immediately after receipt.

26. The method according to claim 25, wherein said validating step includes the steps of

requesting a public key and a digital certificate from the server node by at least one party of the digital agreement;

encrypting a message including said public key and said digital certificate with a private key of a trusted authority, said trusted authority having a public key that is widely disseminated;

transmitting said message to a signatory node of the at least one party;

decrypting said message to obtain said public key;

transmitting a challenge message to the server node requesting a response, said response including a message encrypted with a private key of the server node;

receiving said response by said signatory node; and

decrypting said response with said public key to authenticate the server node.

27. The method according to claim 26, wherein said validating step further includes the step of querying the server node to ascertain information associated with arbitration software contained within the server node.

28. The method according to Claim 24, wherein prior to said receiving step, the method further comprises the step of:

producing said plurality of digital signatures of which each digital signature is unique to one of the plurality of parties, wherein each digital signature of said plurality of digital signatures includes a hash value of the digital agreement encrypted with a private key of a party representative of said digital signature.

29. A server capable of arbitrating execution of a digital agreement involving a plurality of parties, the server comprising:

a bus;

a host processor coupled to said bus;

a memory element coupled to said bus; and

a cryptographic device coupled to said bus, said cryptographic device is capable of receiving a plurality of digitally signed messages from the corresponding plurality of parties, determining whether each of said plurality of digitally signed messages is valid, and transmitting said plurality of digitally signed messages to each of the plurality of parties upon receiving each of said plurality of messages and determining that each of said plurality of messages is valid.

30. The server according to claim 29, wherein said cryptographic device includes

an internal bus;

a processing unit coupled to said internal bus;

a memory element coupled to said internal bus, said memory element contains at least a public key, a private key and arbitration software which, when executed by said processing unit, enables said server to at least determining whether each of said plurality of digitally signed messages is valid; and

a bus control unit coupled to said bus and said internal bus.

31. The server according to claim 29, wherein said cryptographic device is dedicated to exclusively operate as control arbitration between said plurality of parties.

32. A server capable of arbitrating execution of a digital agreement involving a plurality of parties, the server comprising:

a bus;

a memory element coupled to said bus, said memory element containing software configured to respond to an authentication message and to arbitrate execution of the digital agreement; and

a host processor coupled to said bus, said host processor executing said software to at least determine whether a plurality of digitally signed messages from the corresponding plurality of parties is valid.

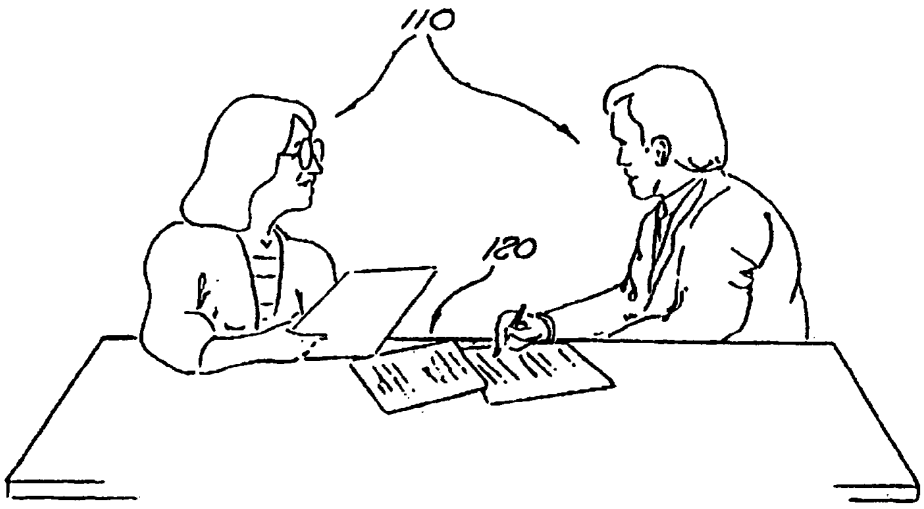


FIG. 1
PRIOR ART

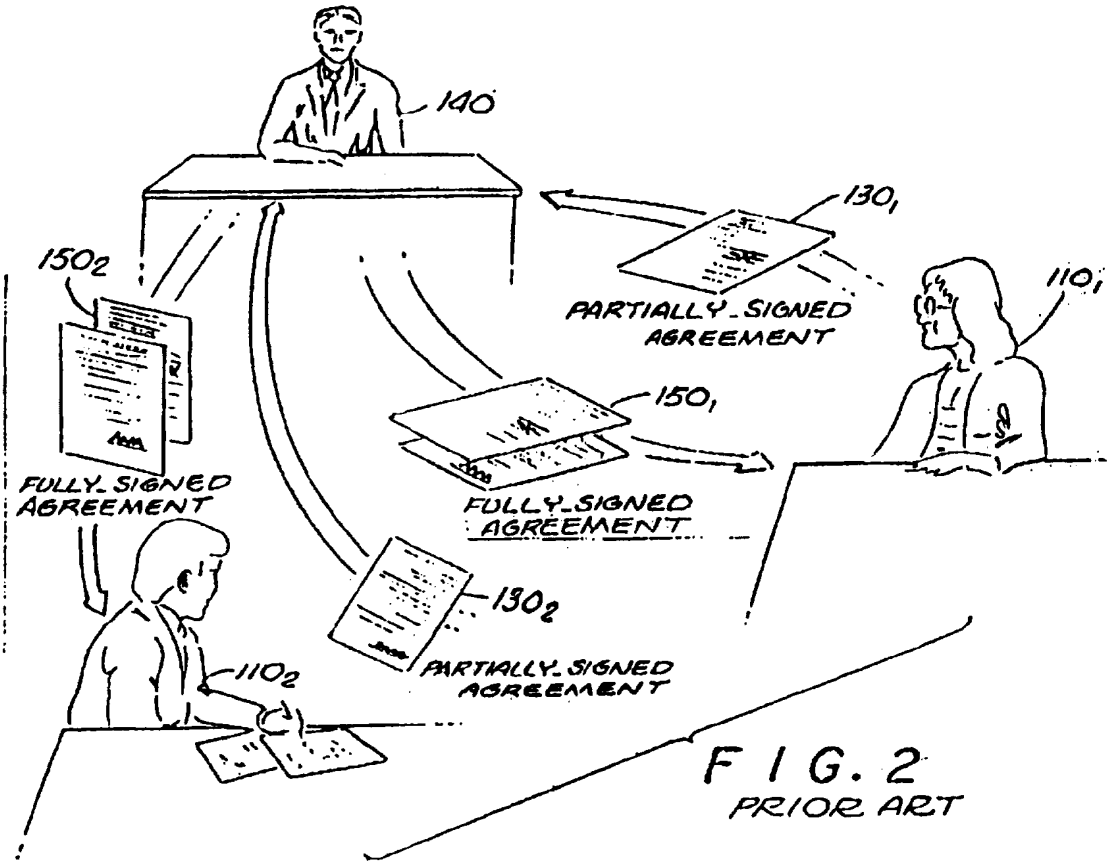


FIG. 2
PRIOR ART

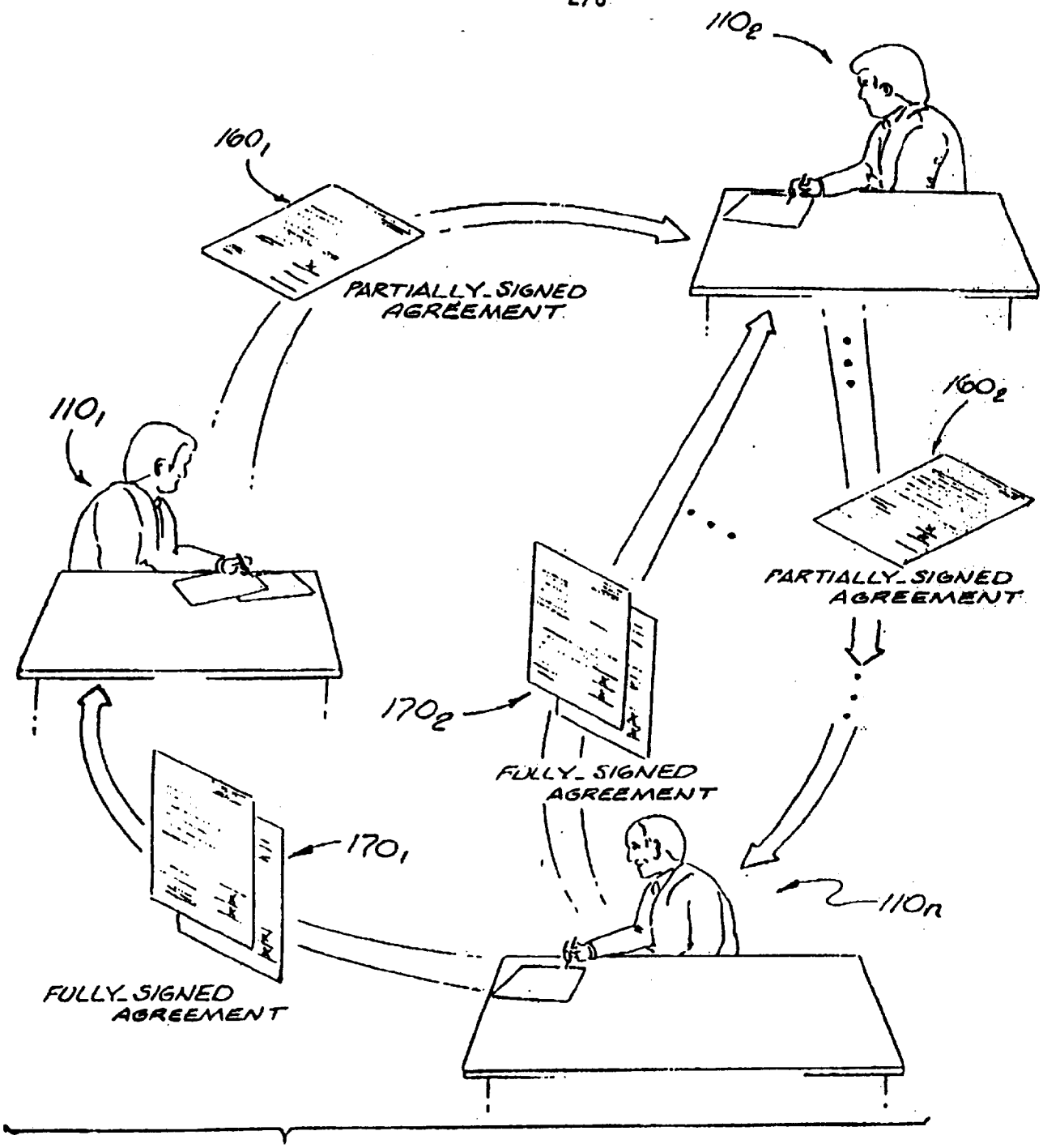


FIG. 3 PRIOR ART

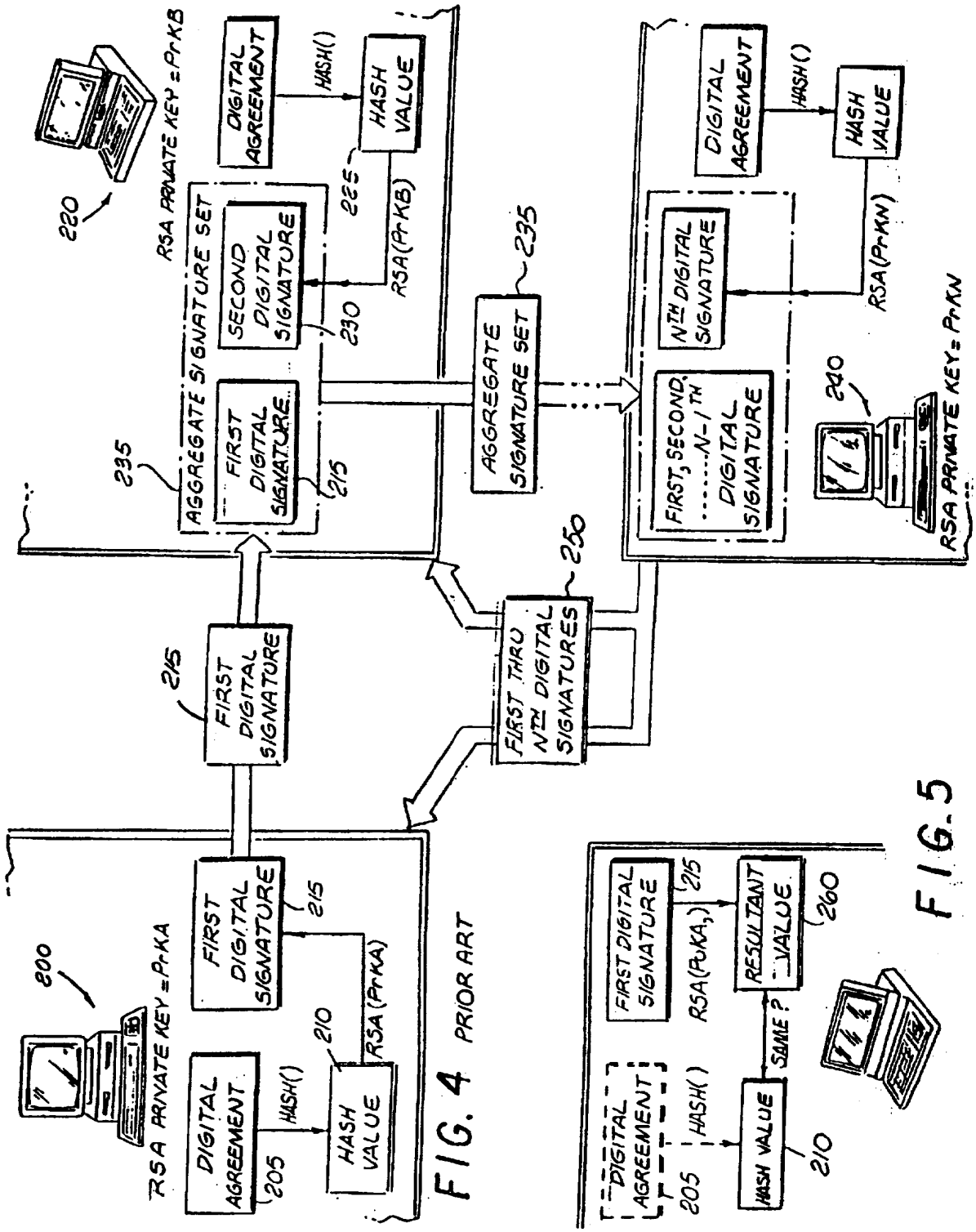
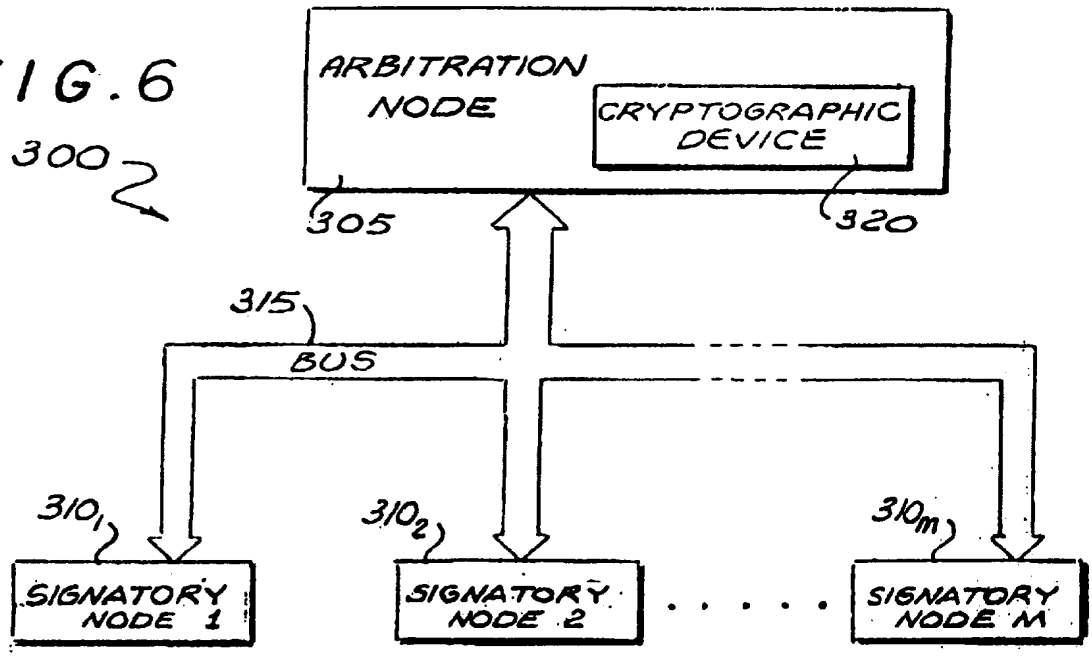


FIG. 4 PRIOR ART

FIG. 5

FIG. 6


300
ARBITRATION NODE
CRYPTOGRAPHIC DEVICE
305
320
315
BUS
310$_1$
310$_2$
310$_m$
SIGNATORY NODE 1
SIGNATORY NODE 2
SIGNATORY NODE M

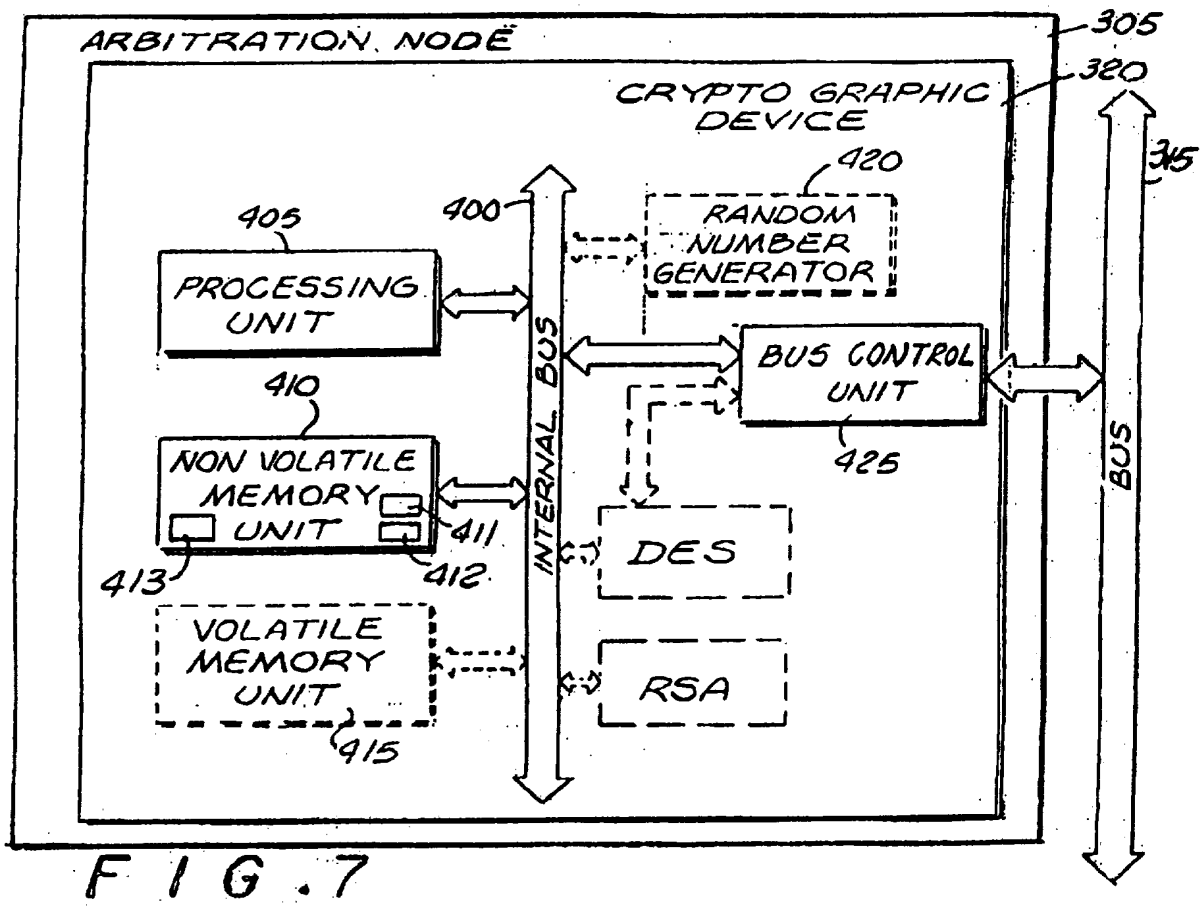

ARBITRATION NODE
305
CRYPTO GRAPHIC DEVICE
320
315
420
400
405
RANDOM NUMBER GENERATOR
PROCESSING UNIT
INTERNAL BUS
BUS CONTROL UNIT
410
NON VOLATILE MEMORY UNIT
411
412
413
425
DES
BUS
VOLATILE MEMORY UNIT
415
RSA

FIG. 7

FIG. 9

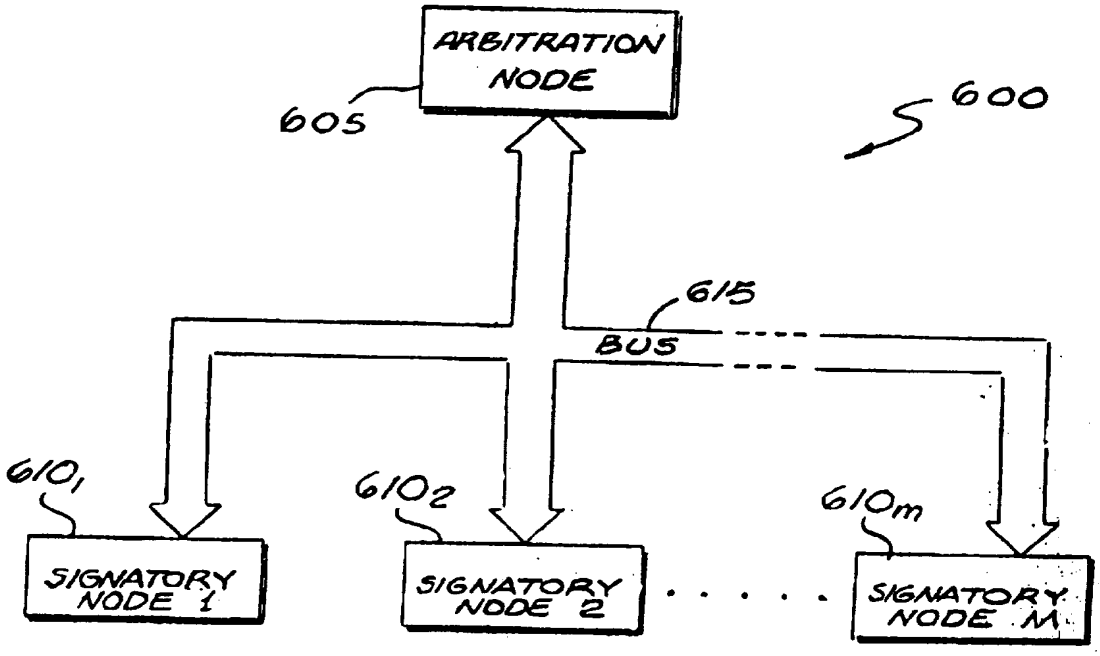

ARBITRATION NODE
605
600
615
BUS
610₁
610₂
610m
SIGNATORY NODE 1
SIGNATORY NODE 2
SIGNATORY NODE M

FIG. 8

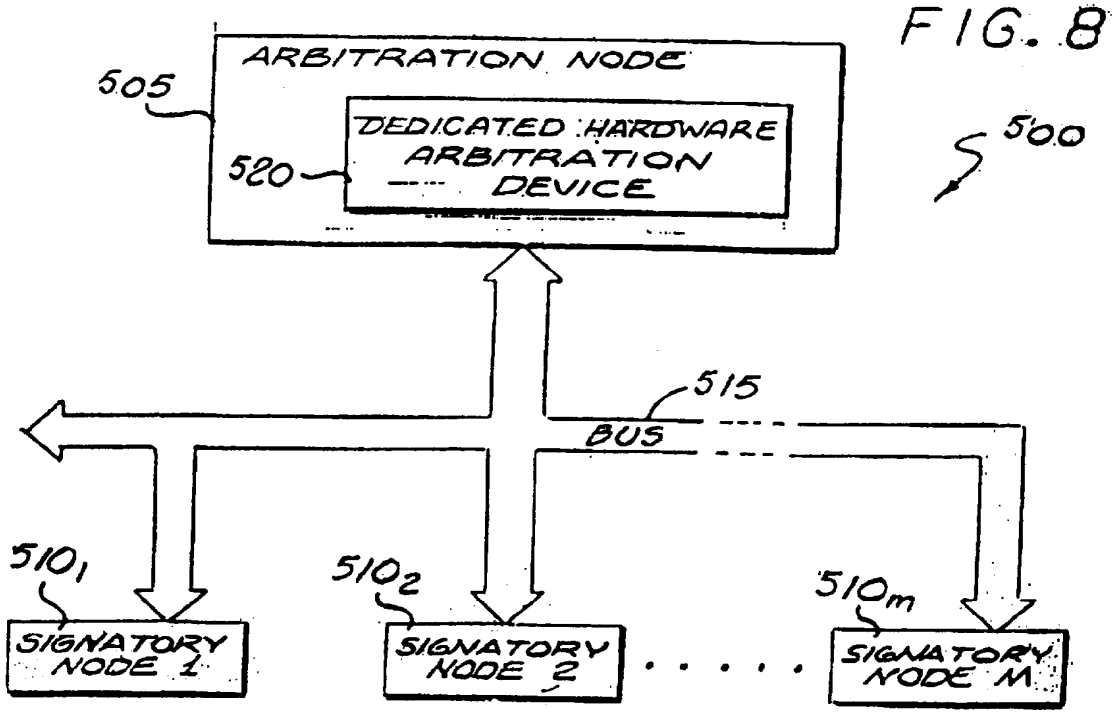
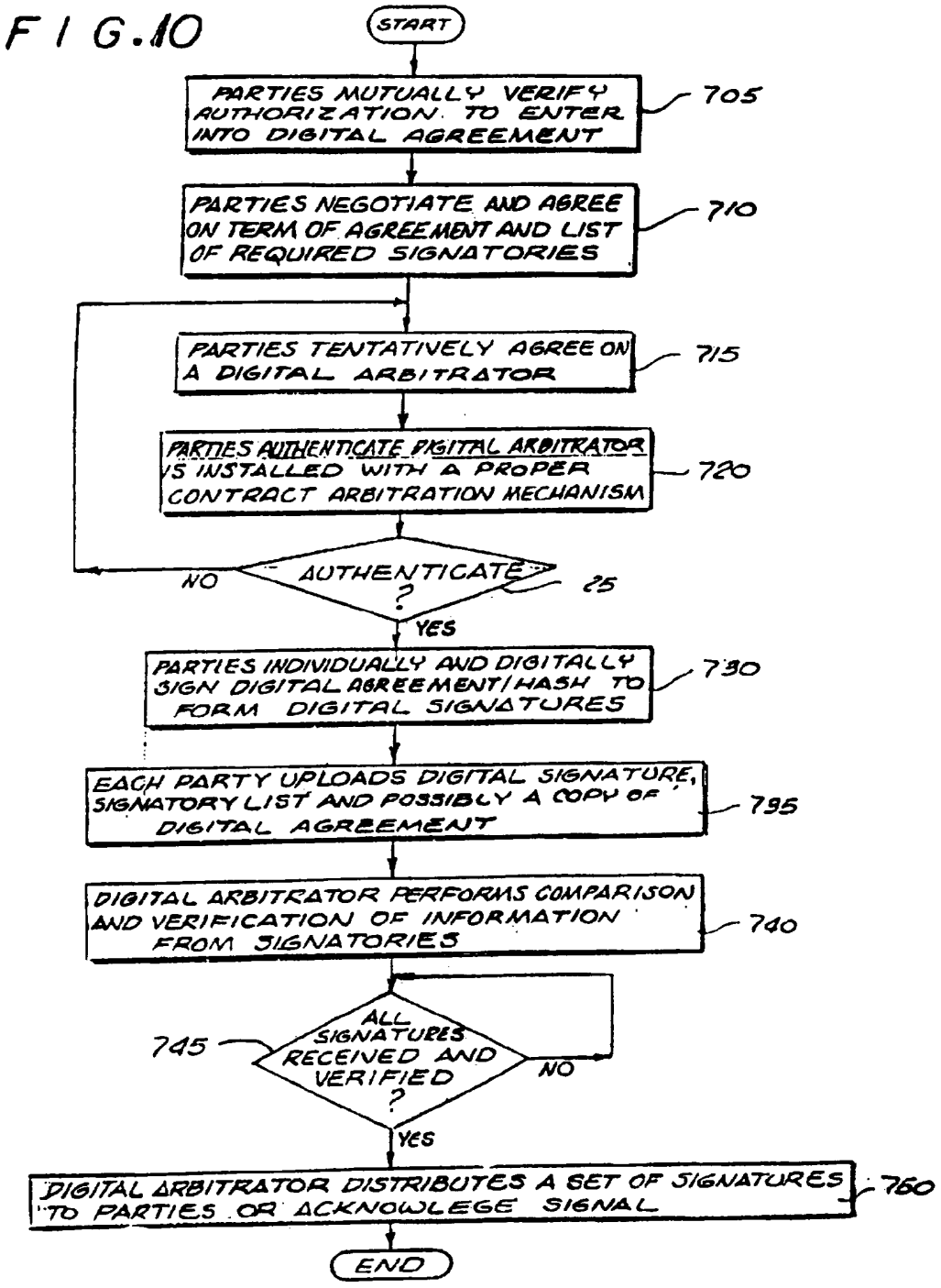

ARBITRATION NODE
505
DEDICATED HARDWARE ARBITRATION DEVICE
520
500
515
BUS
510₁
510₂
510m
SIGNATORY NODE 1
SIGNATORY NODE 2
SIGNATORY NODE M

FIG.10


START
PARTIES MUTUALLY VERIFY AUTHORIZATION TO ENTER INTO DIGITAL AGREEMENT
705
PARTIES NEGOTIATE AND AGREE ON TERM OF AGREEMENT AND LIST OF REQUIRED SIGNATORIES
710
PARTIES TENTATIVELY AGREE ON A DIGITAL ARBITRATOR
715
PARTIES AUTHENTICATE DIGITAL ARBITRATOR IS INSTALLED WITH A PROPER CONTRACT ARBITRATION MECHANISM
720
AUTHENTICATE ?
725
NO
YES
PARTIES INDIVIDUALLY AND DIGITALLY SIGN DIGITAL AGREEMENT/HASH TO FORM DIGITAL SIGNATURES
730
EACH PARTY UPLOADS DIGITAL SIGNATURE, SIGNATORY LIST AND POSSIBLY A COPY OF DIGITAL AGREEMENT
735
DIGITAL ARBITRATOR PERFORMS COMPARISON AND VERIFICATION OF INFORMATION FROM SIGNATORIES
740
ALL SIGNATURES RECEIVED AND VERIFIED ?
745
NO
YES
DIGITAL ARBITRATOR DISTRIBUTES A SET OF SIGNATURES TO PARTIES OR ACKNOWLEGE SIGNAL
760
END

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/10292

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04K 1/00; H04L 9/00; G06F 17/60
US CL :380/25, 364/225, 918; 395/218

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/25, 364/225, 918; 395/218

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS Messenger

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	N, APPLIED CRYPTOGRAPH, BRUCE SCHNEIER, (1ST EDITION), 1994, JOHN SILEY & SONS, INC; See P. 34, 35, 99	1-32
A, E	US, A, 5,666,420 (MICALI) 09 September 1997.	1-32
A, P	US, A, 5,629,982 (MICALI) 13 May 1997.	1-32
A	US, A, 4,881,264 (MERKLE) 14 November 1989.	1-32

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 30 SEPTEMBER 1997	Date of mailing of the international search report 02 DEC 1997
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer STEPHEN C. BUCZINSKI Telephone No. (703) 305-1835

Form PCT/ISA/210 (second sheet)(July 1992)★